<u>What Is Claimed Is</u>:

1.   An electronic data storage system comprising:

a file device for storing at least electronic data; and

5   a data processing unit which generates check codes for detecting falsification respectively for said electronic data and a public key-based electronic signature using a secret encryption method and/or an encryption key when the electronic data is registered, stores said electronic data,

10   said public key-based electronic signature, and said respective check codes, respectively verifies the validity of said stored electronic data and said electronic signature using said check codes attached the stored electronic data and said electronic signature when said electronic data is

15   output, and then accesses said electronic data and said electronic signature.

2.   An electronic data storage system comprising:

a file device for storing at least electronic data; and

20   a data processing unit which generates a check·code for detecting falsification for a public key-based electronic signature using a secret encryption method and/or an encryption key when said electronic data is registered, stores said electronic data, said public key-based electronic

25   signature and the falsification check code for said electronic signature, verifies the validity of said electronic signature using the check code attached to said

21

electronic signature and verifies the validity of said electronic data using said electronic signature when said electronic data is output, and then accesses said electronic data and said electronic signature.

5

3.   The electronic data storage system according to Claim 1, wherein said data processing unit outputs said electronic data with attaching the public key-based electronic signature created at access to the electronic signature at registration to be accessed after verifying the validity of said electronic data and said electronic signature.

4.   The electronic data storage system according to Claim 1, wherein said data processing unit outputs said electronic data with attaching the public key-based electronic signature created at access to the electronic data to be accessed after verifying the validity of said electronic data and said electronic signature.

20

5.   The electronic data storage system according to Claim 2, wherein said data processing unit outputs said electronic data with attaching the public key-based electronic signature created at access to the electronic signature at registration to be accessed after verifying the validity of said electronic data and said electronic signature.

6.   The electronic data storage system according to
Claim 1, wherein said data processing unit stores a
certificate of the public key with which said electronic
5 signature was created, simultaneously along with said
electronic signature, when said electronic signature is
created.

7.   The electronic data storage system according to
10 Claim 1, wherein said data processing unit stores or outputs
the expiration information of said public key certificate
simultaneously.

8.   The electronic data storage system according to
15 Claim 2, wherein said data processing unit stores the
certificate of the public key with which said electronic
signature is created, simultaneously along with said
electronic signature, when said electronic signature is
created.
20

9.   The electronic data storage system according to
Claim 2, wherein said data processing unit stores or outputs
the expiration information of said public key certificate
simultaneously.
25

10.   The electronic data storage system according to
Claim 1, wherein said data processing unit creates a pair of

said public key and said secret key according to the request

for key creation, issues the request of issuing said public

key certificate to a CA office, acquires said public key

certificate, and stores said acquired public key certificate

5   in said file device.

    11.   An electronic data storage method comprising:

    a step of respectively generating check codes for

detecting falsification for electronic data and a public key-

10 based electronic signature using a secret encryption method

and/or an encryption key, when said electronic data is

registered;

    a step of storing said electronic data, said public key-

based electronic signature, and said respective check codes;

15   a step of respectively verifying the validity of said

stored electronic data and said electronic signature using

said check codes attached said stored electronic data and

said electronic signature when said electronic data is

output; and

20   a step of accessing said electronic data and said

electronic signature.

    12.   The electronic data storage method according to

Claim 11, further comprising a step of outputting said

25 electronic signature at registration with attaching a public

key-based electronic signature created at access after

verifying the validity of said electronic data and said

electronic signature.

13. An electronic data storage method, comprising:

a step of generating a check code for detecting

5　falsification for a public key-based electronic signature

using a secret encryption method and/or an encryption key,

when said electronic data is registered;

a step of storing said electronic data, said public key-

based electronic signature, and said falsification check code

10　for said electronic signature; and

a step of verifying the validity of said electronic data

using said electronic data using said electronic signature

after verifying the validity of said electronic signature

using the check code attached to said electronic signature

15　when said electronic data is output, and then accessing said

electronic data and said electronic signature.

14. The electronic data storage method according to

Claim 13, further comprising a step of outputting said

20　electronic signature with attaching a public key-based

electronic signature created at access after verifying the

validity of said electronic data and said electronic

signature.

25　　15. The electronic data storage method according to

Claim 13, wherein output step comprises a step of outputting

said electronic data with attaching a public key-based

electronic signature created at access after verifying the

validity of said electronic data and said electronic

signature.

5   16.   The electronic data storage method according to

Claim 11, wherein said storage step comprises a step of

storing a certificate of the public key with which said

electronic signature was created, simultaneously along with

said electronic signature, when said electronic signature is

10 created.

      17.   The electronic data storage method according to

Claim 13, wherein said storage step comprises a step of

storing a certificate of the public key with which said

15 electronic signature was created, simultaneously along with

said electronic signature, when said electronic signature is

created.

      18.   The electronic data storage method according to

20 Claim 11, wherein said storage or output step comprises a

step of storing or outputting the expiration information of

said public key certificate simultaneously.

      19.   The electronic data storage method according to

25 Claim 11, further comprising a step of creating a pair of

said public key and said secret key according to the request

for the key creation, issuing the request of issuing said

public key certificate to a CA office, acquiring said public key certificate, and storing said public key certificate in said file device.

5   20.   The electronic data storage method according to Claim 13, wherein said storage or output step comprise a step of storing or outputting the expiration information of said public key certificate simultaneously.

10   21.   The electronic data storage method according to Claim 13, further comprising a step of creating a pair of said public key and said secret key according to the request for the key creation, issuing the request of issuing said public key certificate to a CA office, acquiring said public

15 key certificate, and storing same in said file device.

27